Security proposal:

A. Interpret the business’s needs to determine specific information regarding security requirements. Illustrate your response with specific examples. To what extent should unauthorized individuals be prevented from making changes, copying, or deleting files or data on the system? Is there sensitive data for which access must be controlled? What sort of information should be backed up?

B. Then, compare and contrast the options for managing user access to company information. Evaluate each option for its strengths and weaknesses, citing specific evidence that supports your conclusions. Is there a need to have password setups for files? What type of naming conventions should the client use for files and directories? Should individual computer accounts be created? Should everyone have read access to all files?

C. Finally, compare and contrast the options for backing up and storing information, including how often to back up information, storage location, and who should have access to backing up the data. Evaluate each option for its strengths and weaknesses, citing specific evidence that supports your evaluation

**Needs:**

1. UAC:- Standard Users- Every other user in the office would be required to operate on a standard user account, and require administrator approval for any changes to the system. The standard user account controls what your employees can do on your system. It does limit file sharing so you will have to create a shared folder for all creative and design that you want to be shared. Once created by you on the system, I would recommend giving the employees Read/Write capabilities to the folders. This will give the employees access the folder on the network to share or obtain the needed content. I would recommend giving only one administrator account out, until you hire a network administrator for your office.
2. Wireless Security:- WPA2-Enterprise uses the Advanced Encryption Standard which is the best defense against attack. This comes with an 802.1x network will require all users to entire a username and password to access the network. The other options are an open authentication network using implicit deny method, which is still easily hacked. WPA and WEP were older models that use outdated key protection methods and will not provide the necessary security you need.
3. File Encryption:- I would recommend setting up a VPN (Virtual Protected Network) for your two employees who operate outside of your office. VyperVPN will offer the best security and scalability for your business, with up to 30 users on the VPN. Most of the other options are still having issues with intruders stealing vital information on the networks. 43% of cyber attacks target small businesses, settling for second best could be very costly.

Maintenance:

Doing regular maintenance on your network will help immensely in the case of a crash or bug in the system. Doing regular backups of the user data will protect your company from a large file loss. This should be done at least once a week to protect your employees hard work. Some more benefits of using Windows 10 for your business are the automatic system restore points that it creates daily and the File History that allows users to go back and restore accidentally deleted folders or files.

REFERENCES:

<https://www.computerworlduk.com/galleries/smb/best-vpn-for-small-businesses-3671292/>

<https://bestvpn.org/best-vpns-for-small-business/>

<https://www.vpnmentor.com/blog/the-best-vpns-for-multiple-devices-and-connections/>